# Alarm over IP, de zwakste schakel in uw beveiliging?

DDoS-aanvallen, waarbij websites worden overspoeld met dataverkeer, vinden ook in Nederland regelmatig plaats. De aanvallen vormen een zeer groot risico voor de betrouwbaarheid van veel alarmtransmissie-oplossingen die via internet doormelden naar de Particuliere Alarm Centrale (PAC).

**Tekst** Bart Postelmans*

"Het bestellen ven een vliegreis is moeilijker dan het uitvoeren van een DDoS-aanval." Dit zegt Aiko Pras, hoogleraar network operations and management van de Universiteit Twente. "Drie muisklikken en je creditcard, en je kunt een aanval uitvoeren." Dit door de opkomst van speciale websites die deze aanvallen op commando uitvoeren. Het uitvoeren van een DDoS-aanval kan op dat soort websites voor enkele tientjes of voor honderden euro's, afhankelijk van de aanvalscapaciteit. Betalen kan gewoon met een creditcard, maar ook anoniem, met behulp van bitcoins.
"De afgelopen drie jaar zijn die sites in opkomst en sinds een jaar gaat het echt heel snel", zegt beveiligingsonderzoeker Rickey Gevers van RedSocks. Een van die websites voert duizenden aanvallen per dag uit, blijkt uit statistieken die deze site zelf geeft.
"Dit soort websites schiet als paddenstoelen uit de grond", aldus een woordvoerder van de politie. Dat is terug te zien in het aantal DDoS-aanvallen, dat volgens de politie in het afgelopen jaar is gestegen.
"Iedereen die met een computer om kan gaan, kan een DDoS-aanval opzetten. En dat terwijl de gevaren groot kunnen zijn", waarschuwt Pras. "Je kunt een school platleggen, of nog veel meer." Daarom moet er steviger worden opgetreden, stelt hij.

### Groei alarmoverdracht via IP

Van de 500.000 objecten – kantoren, bedrijven en particulieren – die zijn aangesloten op de circa 25 meldkamers of Particuliere Alarm Centrales (PAC's) melden naar schatting inmiddels ruim 140.000 aansluitingen door op basis van het Internet Protocol (alarm over IP). Ruim 25.000 aansluitingen hiervan zijn zogenoemde hogere risico's die tot begin 2015 vanaf de dienst DigiAccess Alarm van KPN zijn overgezet naar IP. Het betreffen hier de zogenoemde AL2/DP3 en AL3/DP4 -locaties, zoals juweliers en bedrijven met aantrekkelijke goederen. Verzekeraars vereisen hier een continue gecontroleerde verbinding met de meldkamer.
DigiAccess Alarm was een speciaal alarmabonnement, waarbij een continu bewaakte, besloten verbinding werd opgezet tussen object en meldkamer. KPN heeft deze alarmdienstverlening 12 januari 2015 definitief uitgezet vanwege verouderde netwerktechnologie. Als vervangende dienst had het bedrijf

> Cybercrime is een onderwerp dat binnen de beveiligingsbranche onvoldoende aandacht heeft

eerder al DigiAlarm geïntroduceerd. Dit is een besloten netwerk dat wel via IP werkt maar geen gebruik maakt van het publieke internet. DigiAlarm voldoet aan de voorschriften van NPR 8136, de Nederlandse Praktijkrichtlijn voor alarmtransmissie via IP-netwerken. Het is als enige alarmtransmissie-oplossing voor de hogere AL2/DP3 en AL3/DP4-risico's door Kiwa end-to-end gecertificeerd conform de Europese norm (NEN-EN 50136).

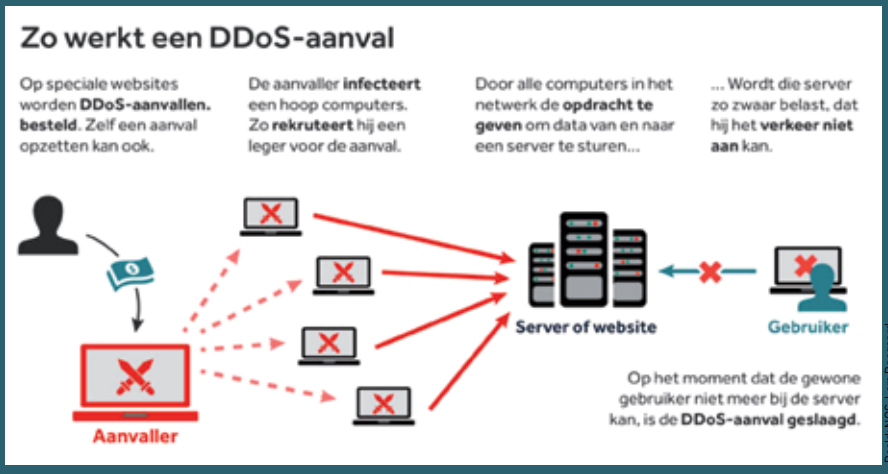
### Beveiligingsbranche

Veel bedrijven hebben de alarmoverdracht naar de meldkamer, vanwege het einde van de DigiAccess Alarm dienstverlening van KPN, laten overzetten op de al aanwezige internetverbinding. Dit op advies van de betrokken alarminstallateur. Hierbij werd en wordt vandaag de dag vaak een zogenoemde VPN-tunnel over internet (VPN: Virtueel Private Netwerk) toegepast met een back-up traject via GPRS met een internet-SIM.
Wat menig installateur niet lijkt te begrijpen of niet te willen begrijpen is dat deze oplossing gewoon doormelding over het publieke internet is, ook wat de ontvangst aan de PAC-zijde betreft. Een hoog-risico locatie zoals bijvoorbeeld een juwelier, die eerder was aangesloten op het veilige en besloten DigiAccess Alarmnetwerk, verstuurt de alarmberichten nu over het publieke internet. Veel 'beveiligingsexperts' lijken geen boodschap te hebben aan het dagelijkse nieuws over cybercriminaliteit zoals DDoS-aanvallen en het hacken van computers en websites.

### DDoS-aanval

Ook in Nederland vinden DDoS-aanvallen op centrale computers en sites regelmatig plaats.

Recent getroffen bedrijven en organisaties zijn onder andere de NOS/websites Publieke Omroep, de Volkskrant, Ziggo en universiteiten zoals die van Leiden en Twente. Toen in augustus Ziggo werd aangevallen lagen circa 2 miljoen internetaansluitingen er bijna twee dagen uit. Objecten die via deze Ziggo internetaansluitingen doormelden naar hun PAC hebben dus bijna 48 uur lang geen primaire alarmdoormelding gehad, met alle risico's van dien.
Ook PAC's kunnen worden getroffen door zo'n DDoS-aanval, waardoor alarmmeldingen van risicolocaties, die op basis van een enkele of tweevoudige internetoplossing doormelden, lange tijd niet bij die meldkamer aankomen. Veel PAC's zijn hier totaal niet op voorbereid. Deze opkomende cybercrime is een onderwerp dat binnen de beveiligingsbranche onvoldoende aandacht heeft.



Beeld: NOS, Lars Boogaard


Van de 500.000 objecten die zijn aangesloten op de circa 25 meldkamers melden naar schatting inmiddels ruim 140.000 aansluitingen door op basis van alarm over IP.

### Kennis installateur

Van alarminstallateurs mag je verwachten dat zij klanten van risicolocaties indringend wijzen op de risico's die ontstaan bij alarmoverdracht over publiek internet. Dat geldt ook voor verzekeraars. Zij behoren bovendien meer zicht te houden op de alarmtransmissiewijzigingen die worden doorgevoerd op hun risicolocaties. Zoals wijzigingen in het 'beveiligd gebied' en het vervallen van de voorkeurschakeling omdat de alarminstallatie gekoppeld moet worden met de router van de IP-aansluiting. Die router staat vaak op een voor iedereen toegankelijke plaats. Wie kan of mag er in die router poorten open en dicht zetten, het IP-nummerplan wijzigen etcetera. Wat gebeurt er bij een stroomstoring als de router uitvalt, is er sprake van een draadloze back-up, is die open over internet of misschien toch besloten en veilig? Nu worden dit soort zaken pas vastgesteld tijdens controles, die zeer beperkt plaatsvinden, of komen ze aan het licht als er een forse schade is.

### NPR 8136

De beveiligingsbranche publiceerde in juli 2012 vanuit NEN (Normcommissie Alarmsystemen - Taakgroep Alarmtransmissie) de Nederlandse praktijkrichtlijn NPR 8136 'Alarmtransmissie over IP-netwerken'. Dit is een leidraad voor het ontwerp, de installatie, de inspectie en het onderhoud, gebaseerd op de Europese norm NEN-EN 50136-1. Zo adviseert men bij lage risico's (AL1/DP1/DP2) tenminste één besloten alarmtransmissieverbinding toe te passen en voor hogere risico's twee besloten verbindingen tussen object en meldkamer te gebruiken. Met 'besloten verbinding' wordt bedoeld een verbinding over een netwerk dat geen gebruik maakt van het internet. Oplossingen die uitgaan van een tunnel (VPN) over internet worden niet als veilig en besloten gekwalificeerd. Dat er vandaag de dag nauwelijks Alarm-over-IP-oplossingen worden aangeboden die NPR-conform zijn, zoals de eerder genoemde DigiAlarm-dienstverlening, is teleurstellend en risicovol. De NPR doet ook aanbevelingen voor de ontvangst-zijde (PAC) zodat bij een DDoS-aanval wordt voorkomen dat dit grootschalige uitval van alarmverbindingen tot gevolg heeft.

### VRKI

Het CCV (Centrum voor Criminaliteitspreventie en Veiligheid) is verantwoordelijk voor de uitgifte en het beheer van de Verbeterde Risico Klasse Indeling (VRKI); dit is 'een instrument om het risico op diefstal te bepalen'.

In het hoofdstuk Alarmering wordt onder andere ingegaan op wat onder een Alarm Transmissie Systeem (ATS) wordt verstaan, de specificatie van de verschillende ATS-categorieën en de prestatieniveaus waaraan moet worden voldaan. Er is ook aandacht voor de verificatie hiervan (VoP) en de beschikbaarheid van het ATS. Dit is inclusief het alarmtransmissienetwerk. Daarbij wordt opgemerkt dat 'ieder beschikbaar netwerk kan worden gebruikt om de meldingen naar de meldkamer te sturen'. Feitelijk is dit juist. Maar, afhankelijk van de risico's zowel op locatie als de sterk groeiende cybercriminaliteit, zou het toch zo moeten zijn dat een netwerk wordt toegepast dat 'voldoende betrouwbaar, veilig en DDoS-ongevoelig' is. Het voor iedereen toegankelijke internet voldoet niet aan deze kwalificatie. Vaak loopt zo'n internetaansluiting met de meldkamer via buitenlandse servers en bedrijven, zonder dat de klant dit weet. De betrouwbaarheid is hierdoor onvoldoende. Bij de VRKI ontbreekt de aandacht voor de opkomende cybercrime. Hier is het nodige werk aan de winkel. De klant moet immers kunnen vertrouwen op de ▶

aangeboden beveiliging en toegepaste veilige alarmtransmissie. Zo ook dat er geen sprake is van schijnbaar goedkope internetoplossingen maar dat direct alle kosten inzichtelijk zijn. Verzekeraars zouden één lijn moeten trekken door vast te houden aan de richtlijnen en adviezen uit de NPR 8136. Uiteindelijk zijn het hun risico's waar een betrouwbare beveiliging wordt vereist, inclusief veilige (besloten) alarmtransmissie-verbindingen met de PAC/ alarmcentrale.

### NEN 8131

NEN 8131 betreft systeem- en kwaliteitseisen plus toepassingsrichtlijnen voor inbraak- en overvalalarmsystemen. De norm geeft regels voor het ontwerp, de uitvoering, de bediening, de inbedrijfstelling, het onderhoud en de kwaliteit van inbraak- en overvalalarmsystemen (afgekort I&OAS). NEN 8131 stelt eisen aan de prestaties van een I&OAS en de kwaliteit van de toegepaste componenten. Daarnaast bevat de norm voorschriften en aanbevelingen voor het ontwerp van het systeem zoals de aard en omvang van de detectie en de wijze van installatie van het systeem. Ook de eisen voor inbedrijfstelling, de documentatie en het onderhoud van een I&OAS staan beschreven in de norm. De eisen en aanbevelingen van NEN 8131 zijn gebaseerd op relevante normen zoals:

- NEN-EN 50131, de Europese normreeks voor alarmsystemen;
- NEN-EN 50136, de normreeks voor alarmtransmissiesystemen.

De systeemeisen en eisen aan apparatuur zijn hieruit overgenomen. Door verwijzing naar deze nieuwe norm kan verouderde regelgeving worden afgeschaft, voor zover deze betrekking heeft op de elektronische beveiligingsmaatregelen. Hierbij valt te denken aan bepaalde onderdelen van de eerder genoemde VRKI van het CCV. Ook de verwijzing naar verouderde voorschriften (gedateerd juli 2000) voor installatie van alarmapparatuur en voorschriften voor beheer en onderhoud van alarmapparatuur van het Verbond van Beveiligingsorganisaties (VvBO, een enkele jaren geleden reeds opgeheven organisatie) is door NEN 8131 overbodig geworden.

Belangrijk gegeven uit de NEN 8131 is dat deze voor wat betreft de alarmtransmissie tussen object en PAC ondubbelzinnig verwijst naar de NPR 8136. Het is hoog tijd dat de NPR 8136 alsook deze NEN 8131 door de beveiligingsbranche als kans op robuustere en betrouwbaardere beveiliging en alarmtransmissie worden gezien. Het negeren hiervan zou, gelet op de cybercrime-risico's, nog wel eens verstrekkende gevolgen kunnen hebben. ■

**Bart Postelmans werkte ruim 33 jaar bij KPN, waar hij verantwoordelijk was voor de introductie van DigiAccess Alarm. Ook was hij betrokken bij de ontwikkeling van Alarm over IP. Van 2007 tot augustus 2015 werkte Postelmans als senior business consultant bij ASB Security in Eindhoven. Eind 2013 droeg KPN de exploitatie van DigiAlarm over aan ASB.*